

Secure ACS per Windows v3.2 con autenticazione computer EAP-TLS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Nozioni di base](#)

[Convenzioni](#)

[Esempio di rete](#)

[Configurazione di Cisco Secure ACS per Windows v3.2](#)

[Ottenere un certificato per il server ACS](#)

[Configurazione di ACS per l'utilizzo di un certificato dall'archivio](#)

[Specificare Autorità di certificazione aggiuntive da considerare attendibili per ACS](#)

[Riavviare il servizio e configurare le impostazioni EAP-TLS su ACS](#)

[Specificare e configurare il punto di accesso come client AAA](#)

[Configurare i database utente esterni](#)

[Riavvia il servizio](#)

[Configurazione della registrazione automatica del computer certificati Microsoft](#)

[Configurazione del Cisco Access Point](#)

[Configurazione del client wireless](#)

[Aggiungi al dominio](#)

[Ottenere un certificato per l'utente](#)

[Configurazione della rete wireless](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene descritto come configurare Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) con Cisco Secure Access Control System (ACS) per Windows versione 3.2.

Nota: l'autenticazione del computer non è supportata con Novell Certificate Authority (CA). ACS può utilizzare EAP-TLS per supportare l'autenticazione del computer in Microsoft Windows Active Directory. Il client utente finale potrebbe limitare il protocollo per l'autenticazione utente allo stesso protocollo utilizzato per l'autenticazione del computer. Ciò significa che l'utilizzo di EAP-TLS per l'autenticazione dei computer potrebbe richiedere l'utilizzo di EAP-TLS per l'autenticazione degli utenti. Per ulteriori informazioni sull'autenticazione dei computer, fare riferimento alla sezione

[Machine Authentication](#) del manuale *utente di Cisco Secure Access Control Server 4.1*.

Nota: quando si imposta ACS per l'autenticazione dei computer tramite EAP-TLS e ACS è stato impostato per l'autenticazione dei computer, il client deve essere configurato per eseguire solo l'autenticazione dei computer. Per ulteriori informazioni, vedere [Come attivare l'autenticazione basata solo sul computer per una rete basata su 802.1X in Windows Vista, Windows Server 2008 e Windows XP Service Pack 3](#).

[Prerequisiti](#)

[Requisiti](#)

Non sono previsti prerequisiti specifici per questo documento.

[Componenti usati](#)

Le informazioni fornite in questo documento si basano sulle versioni software e hardware riportate di seguito.

- Cisco Secure ACS per Windows versione 3.2
- Servizi certificati Microsoft (installato come Autorità di certificazione radice dell'organizzazione [CA])**Nota:** per ulteriori informazioni, consultare la [Guida dettagliata all'impostazione di un'Autorità di certificazione](#) .
- Servizio DNS con Windows 2000 Server con Service Pack 3 e [hotfix 323172](#)**Nota:** se si verificano problemi con il server CA, installare l'[hotfix 323172](#) . Il client Windows 2000 SP3 richiede l'[hotfix 313664](#) per abilitare l'autenticazione IEEE 802.1x.
- Cisco Aironet serie 1200 Wireless Access Point 12.01T
- IBM ThinkPad T30 con Windows XP Professional e Service Pack 1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

[Nozioni di base](#)

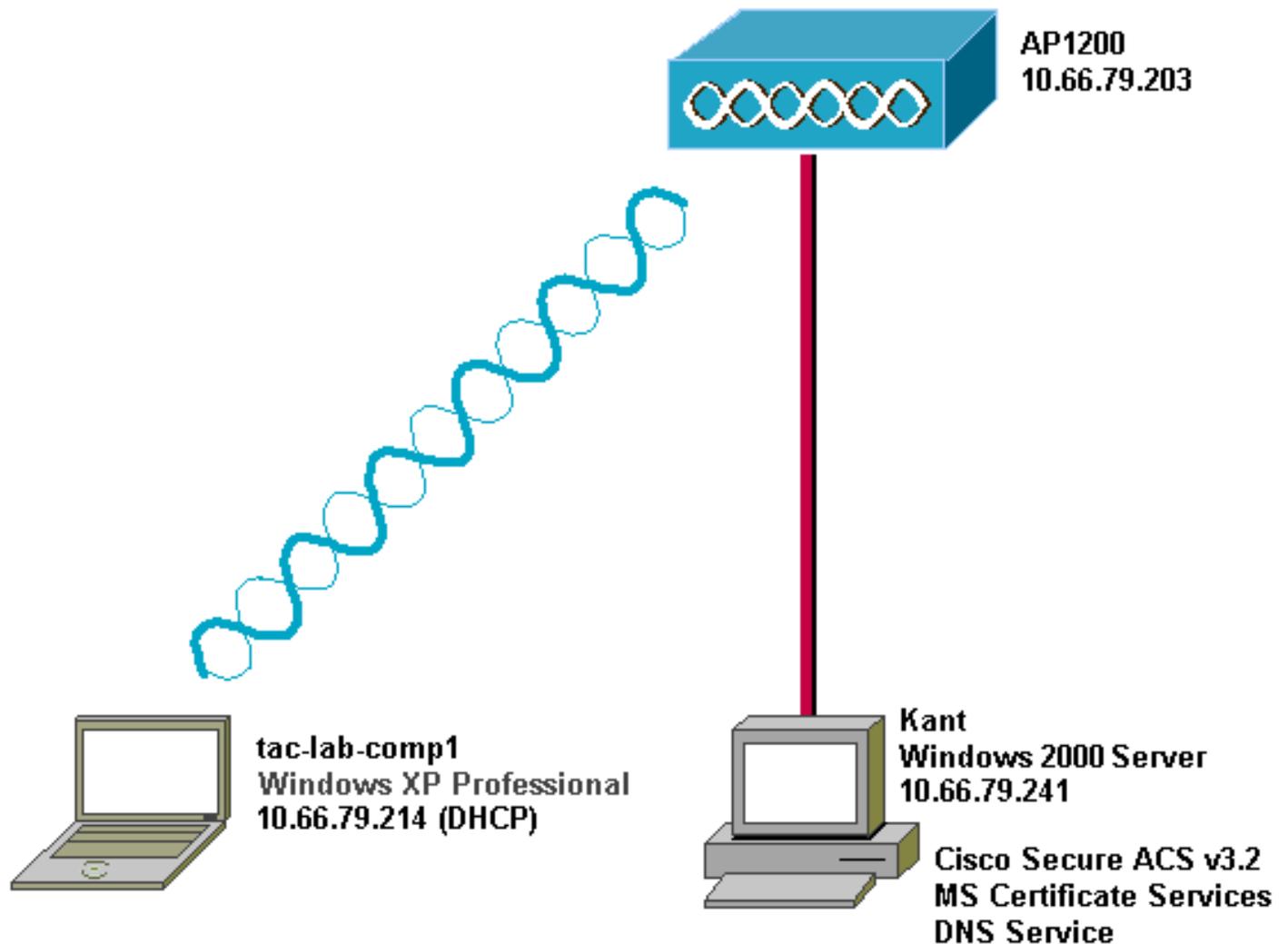
Sia EAP-TLS che PEAP (Protected Extensible Authentication Protocol) generano e utilizzano un tunnel TLS/Secure Socket Layer (SSL). EAP-TLS utilizza l'autenticazione reciproca in cui sia il server ACS (Authentication, Authorization, and Accounting [AAA]) che i client dispongono di certificati e si scambiano le rispettive identità. PEAP, tuttavia, utilizza solo l'autenticazione sul lato server; solo il server dispone di un certificato e ne dimostra l'identità al client.

[Convenzioni](#)

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

[Esempio di rete](#)

Questo documento utilizza le impostazioni di rete mostrate nel diagramma sottostante.



Configurazione di Cisco Secure ACS per Windows v3.2

Per configurare ACS 3.2, procedere come segue.

1. [Ottenere un certificato per il server ACS.](#)
2. [Configurare ACS per l'utilizzo di un certificato di archiviazione.](#)
3. [Specificare le autorità di certificazione aggiuntive da considerare attendibili per ACS.](#)
4. [Riavviare il servizio e configurare le impostazioni PEAP su ACS.](#)
5. [Specificare e configurare il punto di accesso come client AAA.](#)
6. [Configurare i database utente esterni.](#)
7. [Riavviare il servizio.](#)

Ottenere un certificato per il server ACS

Per ottenere un certificato, eseguire la procedura seguente.

1. Sul server ACS, aprire un browser Web e immettere **http://CA-ip-address/certsrv** per accedere al server CA.
2. Accedere al dominio come

Enter Network Password [?] [X]

 Please type your user name and password.

Site: 10.66.79.241

User Name: Administrator

Password: *****

Domain: SEC-SYD

Save this password in your password list

OK Cancel

amministratore.

3. Selezionare **Richiedi certificato** e quindi fare clic su

Microsoft Certificate Services -- Our TAC CA [Home](#)

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

Next >

Avanti.

4. Selezionare **Richiesta avanzata**, quindi fare clic su

Choose Request Type

Please select the type of request you would like to make:

User certificate request:

A rectangular selection box with a blue header containing the text "User Certificate". The main body of the box is empty.

Advanced request

Next >

Avanti.

5. Selezionare **Invia una richiesta di certificato a questa CA utilizzando un modulo**, quindi fare clic su

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

- Submit a certificate request to this CA using a form.
- Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.
- Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

Next >

Avanti.

6. Configurare le opzioni del certificato: Selezionare **Server Web** come modello di certificato e immettere il nome del server

Advanced Certificate Request

Certificate Template:

Web Server

Identifying Information For Offline Template:

Name: OurACS
E-Mail:
Company:
Department:
City:
State:
Country/Region: US

ACS.

Imm

ettere **1024** nel campo Dimensione chiave e selezionare le caselle di controllo **Contrassegna le chiavi come esportabili** e **Usa archivio locale**. Configurare altre opzioni in base alle esigenze e quindi fare clic su

Key Options:

CSP:

Key Usage: Exchange Signature Both

Key Size: Min: 384 Max: 1024 (common key sizes: [512](#) [1024](#))

Create new key set
 Set the container name

Use existing key set

Enable strong private key protection

Mark keys as exportable
 Export keys to file

Use local machine store
You must be an administrator to generate a key in the local machine store.

Additional Options:

Hash Algorithm: Only used to sign request.

Save request to a PKCS #10 file

Attributes:

Invia.

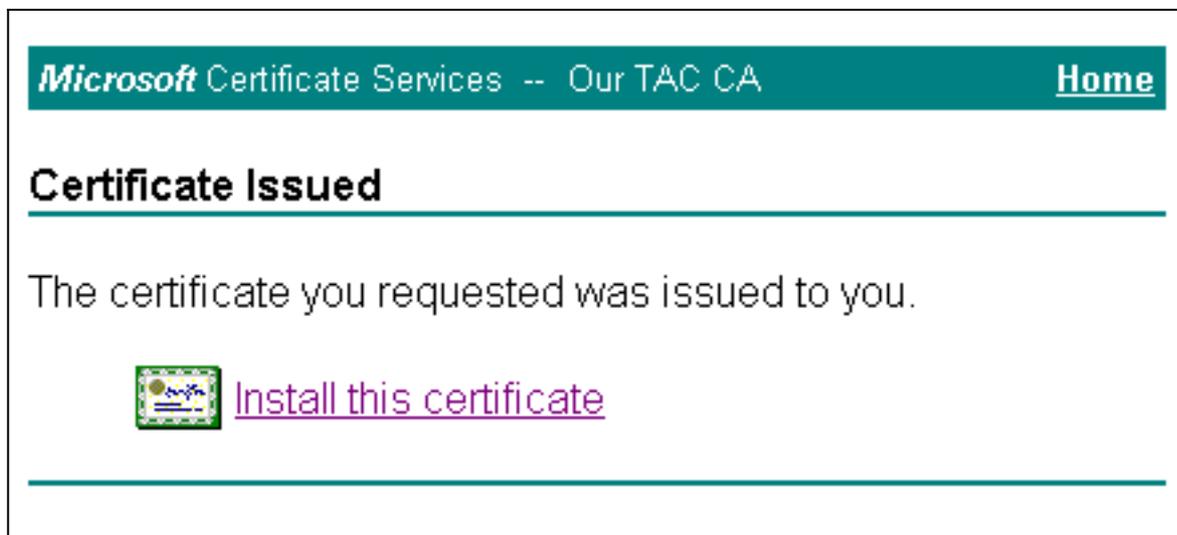
Nota

: se viene visualizzata la finestra di dialogo Potenziale violazione script, fare clic su **Sì** per



continuare.

7. Fare clic su **Installa il**



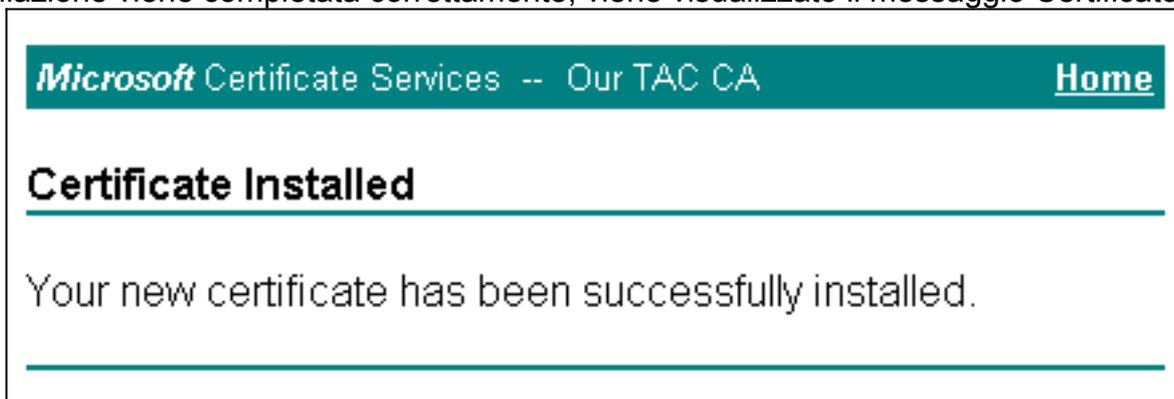
certificato.

Nota: se viene visualizzata la finestra di dialogo Potenziale violazione script, fare clic su **Sì**



per continuare.

8. Se l'installazione viene completata correttamente, viene visualizzato il messaggio Certificato



installato.

[Configurazione di ACS per l'utilizzo di un certificato dall'archivio](#)

Completare questa procedura per configurare ACS in modo che utilizzi il certificato in archiviazione.

1. Aprire un browser Web e immettere **http://ACS-ip-address:2002/a** per accedere al server ACS.
2. Fare clic su **Configurazione di sistema**, quindi su **Configurazione certificato ACS**.
3. Fare clic su **Installa certificato ACS**.
4. Fare clic sul pulsante di opzione **Usa certificato da archiviazione**.
5. Nel campo **Certificato CN**, immettere il nome del certificato assegnato al passaggio 5a di

Ottenere un certificato dalla sezione del server [ACS](#) di questo documento.

6. Fare clic su

The screenshot shows the Cisco System Configuration web interface. On the left is a navigation sidebar with icons and labels for: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration (highlighted with a red border), Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled 'System Configuration' and 'Edit'. Below this is a section titled 'Install ACS Certificate'. Inside this section is a form titled 'Install new certificate' with a help icon. The form contains two radio button options: 'Read certificate from file' and 'Use certificate from storage'. The second option is selected and circled in red. Below the selected option is a text input field for 'Certificate CN' containing the text 'OurACS'. Below this are three more text input fields: 'Private key file', 'Private key', and 'password'. At the bottom of the form is a yellow button with a question mark icon and the text 'Back to Help'. At the very bottom of the page are two buttons: 'Submit' and 'Cancel'.

Invia.

Al termine della configurazione, viene visualizzato un messaggio di conferma che indica che la configurazione del server ACS è stata modificata. **Nota:** al momento non è necessario riavviare

The screenshot shows the Cisco ACS System Configuration interface. On the left is a navigation menu with options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration (highlighted), Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main area is titled 'System Configuration' and 'Edit'. A dialog box titled 'Install ACS Certificate' is open, displaying 'Installed Certificate Information' with the following details:

Issued to:	OurACS
Issued by:	Our TAC CA
Valid from:	June 23 2003 at 02:19:56
Valid to:	June 18 2005 at 00:52:30
Validity:	OK

Below this information is a red warning message: **The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.** At the bottom of the dialog are two buttons: 'Install New Certificate' and 'Cancel'.

L'ACS.

[Specificare Autorità di certificazione aggiuntive da considerare attendibili per ACS](#)

L'ACS considera automaticamente attendibile la CA che ha emesso il proprio certificato. Se i certificati client vengono emessi da CA aggiuntive, completare i seguenti passaggi:

1. Fare clic su **Configurazione di sistema**, quindi su **Configurazione certificato ACS**.
2. Fare clic su **Installazione Autorità di certificazione ACS** per aggiungere le CA all'elenco dei certificati attendibili.
3. Nel campo relativo al file del certificato CA, immettere il percorso del certificato e fare clic su

The screenshot shows the Cisco System Configuration interface. At the top left is the Cisco Systems logo. The main title is "System Configuration". Below the title is a black bar with the word "Edit" in white. On the left side, there is a vertical navigation menu with the following items: "User Setup", "Group Setup", "Shared Profile Components", "Network Configuration", "System Configuration" (highlighted with a red border), "Interface Configuration", "Administration Control", "External User Databases", "Reports and Activity", and "Online Documentation". The main content area is titled "ACS Certification Authority Setup". Below this title is a section titled "CA Operations" with a help icon. The text reads: "Add new CA certificate to local certificate storage". Below this text is a text input field labeled "CA certificate file". At the bottom of the main content area is a yellow button with a help icon and the text "Back to Help".

Invia.

4. Fare clic su **Modifica elenco scopi consentiti ai certificati**.
5. Selezionare tutte le CA che ACS deve considerare attendibili e deselezionare tutte le CA che ACS non deve considerare attendibili.
6. Fare clic su

CISCO SYSTEMS

System Configuration

Edit

Edit Certificate Trust List

Edit the Certificate Trust List (CTL)

Display Name (Friendly Name)

- ABA.ECOM Root CA
(DST (ABA.ECOM) CA)
- Autoridad Certificadora de la Asociacion Na
(Autoridad Certificadora de la Asociacion N)
- Autoridad Certificadora del Colegio Naciona
- Baltimore EZ by DST
(DST (Baltimore EZ) CA)
- Belgacom E-Trust Primary CA
- C&W HKT SecureNet CA Class A
(CW HKT SecureNet CA Class A)
- C&W HKT SecureNet CA Class B
(CW HKT SecureNet CA Class B)

Invia.

[Riavviare il servizio e configurare le impostazioni EAP-TLS su ACS](#)

Completare questa procedura per riavviare il servizio e configurare le impostazioni EAP-TLS:

1. Fare clic su **Configurazione di sistema** e quindi su **Controllo servizio**.
2. Per riavviare il servizio, fare clic su **Restart** (Riavvia).
3. Per configurare le impostazioni EAP-TLS, fare clic su **Configurazione di sistema**, quindi su **Configurazione autenticazione globale**.
4. Selezionare **Consenti EAP-TLS**, quindi controllare uno o più confronti tra certificati.
5. Fare clic su

